Radical Representation of Polynomial Roots

AUTHOR(S):

穴井, 宏和; 横山, 和弘

CITATION:

穴井, 宏和 ...[et al]. Radical Representation of Polynomial Roots. 数理解析研究所講究録 1995, 920: 9-24

ISSUE DATE:

1995-08

URL:

http://hdl.handle.net/2433/59722

数理解析研究所講究録
920巻 1995年 9-24

2.

Radical Representation of Polynomial Roots

穴井 宏和 (富士通情報研)
横山 和弘 (〃)

2.1 数学的基礎

2.1.1 Galois 理論

まず, Galois 理論について簡単に復習する. monic で既約な $\mathbf{Z}$ 上の n 次の多項式を $f(x)$ とする. このとき,$f(x)$ の Galois 群 G は以下のような群の列が存在するときにかぎり可解である.

$$G = G_0 \supset G_1 \supset \cdots \supset G_{r-1} \supset G_r = 1,$$

ここで,G_i は G_{i-1} の正規部分群で各々の G_{i-1}/G_i は素数次数 p_i の巡回群である. この列を組成列 (*composition series*) という. 組成列が存在する, すなわち G が可解であるとすると Galois 対応より体の列

$$\mathbf{Q} = K_0 \subset K_1 \subset \cdots \subset K_{r-1} \subset K_r = K_f,$$

が存在する. ここで, K_f は f の分解体で, K_i は G_i の作用の下で不変であるような全ての元から構成される体である. このとき, K_i は K_{i-1} の巡回 (Galois) 拡大であり, その拡大次数 $|\ K_i : K_{i-1}\ |$ は p_i である. さらに, 各拡大 K_i/K_{i-1} は有限次拡大であるから, $K_i = K_{i-1}(\beta_i)$ なる K_i の原始元 β_i が存在する.

全ての原始元 β_i がベキ根で表されれば, f の全ての根もまたベキ根で表される. よって,Galois 群

G の可解性とは, 体の列における全ての原始元 β_i がベキ根で表されることを意味する. より詳しくいうと次のようになる. ここで,1 の原始 p_i乗根を ζ_{p_i} とする.

1. $\zeta_{p_i} \in K_i$ ならば, $\beta_i^{p_i} \in K_{i-1}$ なる K_i の原始元 β_i が存在する. すなわち,β_i は ある元 $\beta_i^{p_i}$ の p_i乗根である.

2. $\zeta_{p_i} \notin K_i$ ならば, $L_{i-1} = K_{i-1}(\zeta_{p_i})$, $L_i = K_i(\zeta_{p_i})$ とする. そのとき,$\beta_i^{p_i} \in L_{i-1}$ なる L_i の原始元 β_i が存在する.

素数 p にたいして, 全ての 1 の原始 p 乗根はベキ根表現可能なので, ひとたび β_i がベキ根で表されれば β_{i+1} もベキ根表現できる. 最終的に K_r の原始元がベキ根表現され K_r 上の f の全ての根のベキ根表現ができる.

したがって, 多項式の根のベキ根表現の問題は, 巡回拡大の原始元のベキ根表現の問題へと帰着される.

2.1.2 巡回拡大

巡回拡大の場合のベキ根表現の方法について, 代数の教科書 [18] [14] 等で見られる Lagrange の分解式 (*resolvent*) に基づいた標準的な方法を見よう.

巡回拡大 $K(\beta)/K$ を考える. K は体で, 拡大次数 $|K(\beta) : K|$ を n とし, σ を その Galois 群 G の生成元とする. すなわち,$G = \{1, \sigma, \cdots, \sigma^{n-1}\}$.

K 上の β のベキ根表現に向けて, 必要なのは $K(\beta)$ の元 γ で, γ は原始元でもあり $\gamma^n \in K$ なる元である. もしこのような元 γ が見つかれば, β は K 上 γ の多項式として表されるからである. 実は,Lagrange の分解式はこの性質をもち, さらに効率的に計算可能なのである.

以下, 基礎体 K は 1 の原始 n 乗根を含んでいるとし, n は K の標数 (*characteristic*) によって割れないとする. この仮定の下で次の良く知られた命題が成立する.

命題 1 K の元で $x^n - a$ が既約多項式で $x^n - a$ のどの根も $K(\beta)$ の原始元になるような元 a が存在する. さらに, 元 $\gamma \in K(\beta)$ は, ある 1 の原始 n 乗根 ζ に対して$\sigma(\gamma) = \gamma\zeta$ が成立するときに限り, $K(\beta)$ の原始元かつ γ^n は K に属する.

$K(\beta)$ の原始元 β に対して, Lagrange の分解式は

$$\begin{aligned} u(\beta, \zeta) &= \beta + \zeta\sigma(\beta) + \cdots + \zeta^{n-1}\sigma^{n-1}(\beta) \\ &= \beta_0 + \zeta\beta_1 + \cdots + \zeta^{n-1}\beta_{n-1}, \end{aligned} \tag{1}$$

で与えられる. ここで,ζ は 1 の n 乗根 (かならずしも原始ではない) で$\beta_\nu = \sigma^\nu(\beta)$, $\sigma(\beta_\nu) = \beta_{\nu+1}$ $(\beta_n = \beta_0)$. (β は原始元なので $\beta_1, \cdots, \beta_{n-1}$ は次数は n より小さい β の多項式として表される.) このとき,

$$\sigma(u(\beta, \zeta)) = \beta_1 + \zeta\beta_2 + \cdots + \zeta^{n-2}\beta_{n-1} + \zeta^{n-1}\beta_0 \tag{2}$$

$$= \zeta^{-1}(\beta_0 + \zeta\beta_1 + \cdots + \zeta^{n-1}\beta_{n-1})$$
$$= \zeta^{-1}u(\beta,\zeta).$$

よって, n 乗 $u(\beta,\zeta)^n$ は σ の作用の下で不変であり, $u(\beta,\zeta)^n$ は基礎体 K に属する. さらに,$u(\beta,\zeta) \neq 0$ なる 1 の原始 n 乗根 ζ が存在すれば (そういう 1 の原始 n 乗根 ζは存在する (補題 9)), ζ^{-1} もまた 1 の原始 n 乗根なので, $u(\beta,\zeta)$ は $K(\beta)/K$ の原始元である.

それゆえ, この場合 $P(u(\beta,\zeta)) = \beta$ なる K 上の多項式 $P(x)$ が存在する. これより,K 上の β のベキ根表現が得られる.

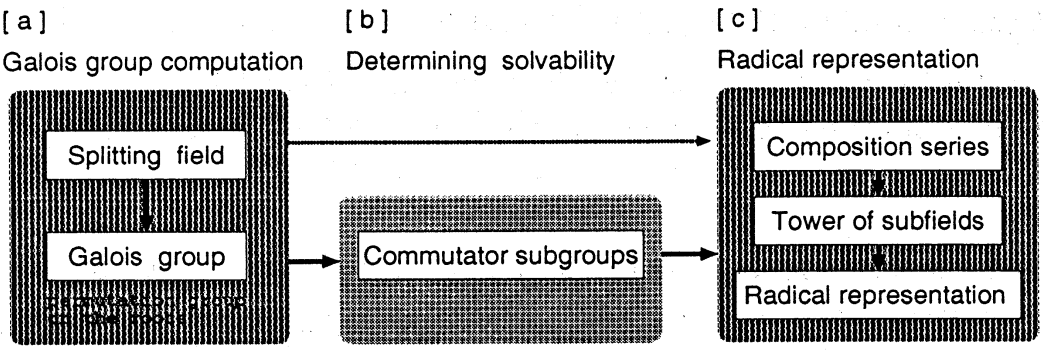
他に教科書等で見られるものとして, 全ての n 乗根 ζ に対する Lagrange の分解式 $u(\beta,\zeta)$ を用いた以下のような記述がある. ζ^{-r} を (1) 式に掛けて全ての 1 の n 乗根 ζ について和をとると,

$$\sum_{\zeta} \zeta^{-r}u(\beta,\zeta) = n\beta_r \tag{3}$$

したがって, $u(\beta,\zeta)$ がわかれば n は K の標数によって割れないので (3) から β_r が求まる. そして, β は $u(\beta,\zeta)$ (これらは全て K の元の n 乗根) の K-線形和 として表される.

2.2 概要

多項式の根のベキ根表現は以下のような (a)(b)(c) 3 部構成になっている. ただし, 冒頭でも述べたとおりここでは (c) について着目している. (c) においては前節の議論から, (i) Galois 群の組成列の構成 (ii) 組成列に対応した部分体の列の構成 (iii) 各拡大の原始元のベキ根表現の構成 という手順が必要である. 根をベキ根で表すことが目的であるので Galois 群は根の上の置換群として具体的に求める必要がある. よって (a) については [3] の direct method を用いる. したがって,(c) に進む前には, 与えられた既約多項式 $f(x)$ に対し, その分解体 K_f は剰余環として, また Galois 群 G は $f(x)$ の根 $\alpha_1,\cdots,\alpha_n$ の上の置換群として求まっている. (根といっても, 全ての根はある変数に割り当てられている.)



具体的には以下のような状況が設定される (詳細は [3] 参照);

分解体 $K_f \simeq \mathbf{Q}(\alpha_1,\cdots,\alpha_n)$ は剰余環 $\mathbf{Q}[y_1,\cdots,y_n]/\mathcal{J}$ により表される. ここで, 各根 α_i, $i=1,\cdots,n$ は変数 y_i に割り当てられ, $\mathcal{J}$ は, α_i の間の全ての代数関係からなるイデアルで極大である. このイデアル $\mathcal{J}$ を K_f の 定義イデアル (*defining ideal*) という. $\mathcal{J}$ は定義多項式 (*defining polynomials*) $\{f_1(y_1), f_2(y_1,y_2),\cdots,f_n(y_1,\cdots,y_n)\}$ により生成される. ここで, 各 $f_i(y_1,\cdots,y_i)$ は, y_i について monic で $f_i(\alpha_1,\cdots,\alpha_i)=0$ となる. また, $f_i(y_1,\cdots,y_i)$ は拡大体 $\mathbf{Q}[y_1,\cdots,y_{i-1}]/\langle f_1,\cdots,f_{i-1}\rangle$ 上で y_i について monic で既約な多項式である. (以降, 多項式の集合 P に対して $\langle P\rangle$ は P によって生成されるイデアルを表すとする.) G は f の根 $y_1,\cdots,y_n$ 上の置換群として表されている. direct method を用いると, その中で $\mathbf{Q}$ 上の K_f の原始元 β は根の $\mathbf{Z}$-線形和として求まっている. それを $\beta=a_1\alpha_1+\cdots+a_n\alpha_n$ $(a_i\in\mathbf{Z})$ とする.[3] より, $K_f=\mathbf{Q}(\alpha_1,\cdots,\alpha_\ell)$ なる整数 ℓ $(\leq n)$ が存在し, 長さ (*length*) という. このとき, β において $a_{\ell+1}=\cdots=a_n=0$ としてよく, また,$i=\ell+1,\cdots,n$ に対しては A_i を多項式として $f_i=x_i-A_i(x_1,\cdots,x_\ell)$ となる. またこのとき, Galois 群の各元の作用は $\alpha_1,\cdots,\alpha_\ell$ の上の作用できまることから, 余分な変数 $y_{\ell+1},\cdots,y_n$ を省いても良いことがわかる. したがって, $K_f\equiv\mathbf{Q}[y_1,\cdots,y_\ell]/\langle f_1(y_1),\cdots,f_\ell(y_1,\cdots,y_\ell)\rangle$. よって, 以下 $y_1,\cdots,y_t$ によって $y_1,\cdots,y_n$ あるいは $y_1,\cdots,y_\ell$ を表すことにする.

(b) の Galois 群の可解性の判定については, 群論に関する既存のアルゴリズムを用いる. ここでは解説は省略する.(詳しくは [1] [4] を参照.) さらに, 群の組成列の計算についても dominant な部分ではないこともあり, 既存の方法 ([5], [8], [11]) を用いる. 以後, 組成列もすでにわかっているとする.

2.3 部分体の構成

既存の置換群のアルゴリズムを使って組成列 ; $G_0=G,G_1,\cdots,G_r=1$, が構成されたとする. すなわち, 組成列の各剰余群 G_{i-1}/G_i, $i=1,\cdots,r$ は, 位数が素数 p_i の巡回群であるとする. このとき, 組成列に対応する部分体の列を構成する. 部分体はそれぞれ各原始元 β_i と最小多項式として与えられる.

まず, ある原始元 β を含む G_i の軌道 (*orbit*) を B_i とする. すなわち,$B_i=\{\sigma(\beta)\mid\sigma\in G_i\}$. β は原始元だから B_0 は K_f 中の β の全ての共役元の集合であり,G は B_0 に正則に作用する. これより,$|B_i|=|G_i|=|K_f:K_i|=|K_f:\mathbf{Q}|/|K_i:\mathbf{Q}|$. 各 B_i に対して以下を考える.

定義 1 K_f の有限集合 B に対して, 多項式 f_B は以下のように定義される.

$$f_B=\prod_{b\in B}(x-b)$$

f_B を B に対応した多項式 (polynomial corresponding to B) という. さらに,K_B を f_B の全ての係数を $\mathbf{Q}$ に添加して得られる体とする. そのとき, K_B は K_f の部分体である. K_B を B に対応する体 (field corresponding to B) という.

軌道 $B_1,\cdots,B_r$ にそれぞれ対応した部分体 $K_{B_1},\cdots,K_{B_r}$ を考えと, 直ちに次を得る.

補題 2各 i に対して,K_{B_i} は K_i と一致する.

$p_i=|K_{i-1}:K_i|$ が素数なので K_i と K_{i-1} の間には真の部分体は存在しない. これと,[19] とより次が成立する.

系 3 f_{B_i} の係数の集合の中に K_{i-1} 上の K_i の原始元が存在する. さらに, K_{i-1} に属さない f_{B_i} の係数はすべて K_{i-1} 上の K_i の原始元となる.

K_{i-1} 上の原始元と $\mathbf{Q}$ 上の原始元とことなることがあるので, 以下を定義しておく.

定義 2 K_{i-1} 上の K_i の原始元を 逐次 *(successive)* 原始元, K_{i-1} 上の K_i の原始元でまた,$\mathbf{Q}$ 上の K_i の原始元でもあるとき絶対的 *(absolutely)* 原始元という.

注意 1明らかに, $f_{B_r}=x-\beta$ なのでβ は K_{r-1} 上の $K_f=K_r$ の最後の原始元であり, 絶対的原始元である. また, K_{r-1} 上の $K_f=K_r$ の最後の原始元として与えられた多項式のある根を選べる.

補題 4全ての根 $\alpha_1,\cdots,\alpha_n$ *(*特に $\alpha_1,\cdots,\alpha_\ell$*)* のうち, K_{r-1} に属さない根 α_j が存在する. このとき, この α_j は K_{r-1} 上の $K_f=K_r$ の逐次原始元である. さらに,G_{r-1} が $G_0=G_f$の正規部分群であれば, 全ての根 α_i もまた K_{r-1} 上の $K_f=K_r$ の逐次原始元である.

以上より, 部分体を計算するアルゴリズムが完成する. まず,$K_1,\cdots,K_i$ はすでに得られているとする. すなわち, 各原始元 β_j, $1\le j\le i$, はそれぞれ f_{B_j} の係数として得られているとする. このときに, 次の K_{i+1} の原始元 β_{i+1} を求める. 系 3 あるいは 補題 4よりβ_{i+1} は $f_{B_{i+1}}$ の係数で K_i に属さないもの, あるいは,K_i に属さない根として選ばれる. そのような元を見つけるのには, $\beta_1,\cdots,\beta_i$ と β_{i+1} の候補となる係数あるいは根の間の代数関係求めればよい. これは,Gröbner 基底の方法を用いれば容易に計算できる. まとめると,

アルゴリズム 1 *Next Successive Primitive Element*

Input: G_{i+1}, β, $\beta_1,\cdots,\beta_i$.

Output: β_{i+1}, $m_{i+1}(x;\beta_1,\cdots,\beta_i)$.

1. $f_{B_{i+1}}$ を計算する.
2. $f_{B_{i+1}}$ の係数のうち K_i に含まれない係数 c を見つける.
3. K_i 上の c の最小多項式を$\beta_1,\cdots,\beta_i$ と c の間の最小次数 d *(*$=p_{i+1}$*)* の代数関係として求める. すなわち,

$$c^d+m_{d-1}(\beta_1,\cdots,\beta_i)c^{d-1}+\cdots+m_0(\beta_1,\cdots,\beta_i)=0,$$

ここで,$m_0,\cdots,m_{d-1}$ は $\mathbf{Q}$ 上の $\beta_1,\cdots,\beta_i$ の多項式である.

4. c を β_{i+1} として, また $c^d+\cdots+m_0$ を $m_{i+1}(x_i;\beta_1,\cdots,\beta_i)$ として出力.

$i=r-1$ のとき, ステップ *1, 2* を次の ステップ *1′* で置き換えてもよい.

1′. $f(x)$ の全ての根のうち K_{r-1} に含まれない根 c を見つける.

絶対的原始元の場合も同じような手順で次の原始元を構成する方法 ([4] 参照) が考えられるが, 実際の

計算の効率は逐次表現の方が優れていることもあり, これ以降は 逐次表現の方についてだけ述べることにする. 具体的な方法を述べる前にここで次を仮定する.

仮定 1逐次原始元 $\beta_1,\cdots,\beta_{i-1}$ は既に得られているとする. ここで, 各 β_j, $j=1,\cdots,i-1$ は $\mathbf{Q}$ 上の $y_1,\cdots,y_t$ の多項式である. $K_{j-1}=\mathbf{Q}(\beta_1,\cdots,\beta_{i-1})$ 上のβ_j の最小多項式 $m_j(x)$ もまた $j=1,\cdots,i-1$ に対して得られているとする. $(m_j(x)=m_j(x,\beta_{i-1},\cdots,\beta_1).)$ ここで m_j を 逐次最小多項式という.

方法 1i 番目のステップを考える. まず, ある原始元 β を含む G_i の軌道 B_i を求め対応する多項式 f_{B_i} を計算する. $f_{B_i}(x)=x^{n_i}+f_{i,n_i-1}x^{n_i-1}+\cdots+f_{i,1}x+f_{i,0}$ とする.

原始元の候補となる元 γ を 係数 $f_{i,j}$ あるいは $i=r$ならばある根 α_jから選ぶ. γ が K_{i-1} 上の K_i の原始元であるかどうか基底変換 (basis-conversion) により決める. $u_1,\cdots,u_{i-1},v$ を新しい変数とし, それぞれ $\beta_1,\cdots,\beta_{i-1},\gamma$に割り振る. すなわち,

$$u_j-\beta_j(y_1,\cdots,y_t)=0 \qquad j=1,\cdots,i-1$$
$$v-\gamma(y_1,\cdots,y_t)=0$$

多項式環 $\mathbf{Q}[y_1,\cdots,y_t,u_1,\cdots,u_{i-1},v]$ の $u_1-\beta_1,\cdots,u_{i-1}-\beta_{i-1},v-\gamma,f_1,\cdots,f_t$ で生成されるイデアル $\bar{\mathcal{J}}$ を考える.

$\bar{\mathcal{J}}$ は $\mathbf{Q}[y_1,\cdots,y_t,u_1,\cdots,u_{i-1},v]$ の極大イデアルであり,$\mathbf{Q}[y_1,\cdots,y_t,u_1,\cdots,u_{i-1},v]/\bar{\mathcal{J}}$ は K_f と同型である. また辞書式順序 $y_1\prec\cdots\prec y_t\prec u_1\prec\cdots\prec u_{i-1}\prec v$ について $\{v-\gamma,u_{i-1}-\beta_{i-1},\cdots,u_1-\beta_1,f_t,\cdots,f_1\}$ は (そのままで) $\bar{\mathcal{J}}$ の *Gröbner* 基底である.

一方, 別の順序 *(block order)* $\{\{u_1,\cdots,u_{i-1}\}\prec v\}\prec\prec\{y_1,\cdots,y_t\}$ について$\bar{\mathcal{J}}$ の (簡約) *Gröbner* 基底を求めると, γ が原始元であるかどうか決めることができ, 同時にその最小多項式も求まる.

この方法は以下の定理等によってその正当性が保証される.(証明略. [4] 参照)

定理 5(1) 消去イデアル *(elimination ideal)* $\bar{\mathcal{J}}\cap\mathbf{Q}[u_1,\cdots,u_{i-1}]$ は, $\mathbf{Q}$ 上の逐次最小多項式 $m_1(u_1),\cdots,m_{i-1}(u_{i-1},u_{i-2},\cdots,u_1)$ によって生成される極大イデアルと一致する.

(2) 消去イデアル $\bar{\mathcal{J}}\cap\mathbf{Q}[u_1,\cdots,u_{i-1},v]$ は, 逐次最小多項式 $m_1,\cdots,m_{i-1}$ とγ の $K_{i-1}=\mathbf{Q}(\beta_1,\cdots,\beta_{i-1})$ 上の最小多項式から生成されるイデアルと一致する.

Gröbner 基底の性質より,

系 6$\bar{\mathcal{J}}$ の *block ordering* $\{u_1,\prec\cdots\prec u_{i-1}\prec v\}\prec\prec\{y_1,\cdots,y_t\}$. についての簡略された *Gröbner* 基底 を GB とする.

(1) 各 $j=1,\cdots,i-1$ に対して, GB に K_{j-1} 上の β_jの逐次最小多項式と一致する多項式 $m_j(u_j,u_{j-1},\cdots,u_1)$ が存在する.

(2) GB に $K_{i-1}=\mathbf{Q}(\beta_1,\cdots,\beta_{i-1})$ 上のγ の最小多項式と一致する多項式 $h(v,u_{i-1},\cdots,u_1)$ が存在する.

よって, 変数の順序を変えると K_{i-1} 上の γ の最小多項式が求まり, $\gamma\in K_{i-1}$ かどうかγ の最小多項式が v について 1 次でないかどうかで決定できる.

系 7以下の *(1)(2)* は同値である.

(1) γ は K_{i-1} 上の K_i の逐次原始元である.

(2) GB に $\mathbf{Q}$ 上の $u_1, \cdots, u_{i-1}, v$ の多項式で v について非線形な元が存在する.

2.4 巡回拡大のベキ根表現

さて, 各原始元 β_i, $i = 1, \cdots, r$ のベキ根表現について考えるのであるが, この節ではまず一般の場合に Lagrange の分解式に基づいた巡回拡大のベキ根表現の方法について述べる. この方法は, 零でない Lagrange の分解式を構成する部分と原始元を Lagrange の分解式 とある 1 の原始 p 乗根の多項式として表す部分からなる. 一般の素数次の巡回拡大について以下を設定する.

仮定 2 L を 基礎体 K の拡大次数が素数次 p の巡回拡大とする. K は,$\mathbf{Q}$ あるいは その有限次拡大とする.G をその *Galois* 群とする. このとき,L/K の 原始元 β とその全ての K 上の共役元は与えられているとする.

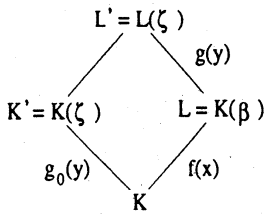
これは,K 上の β の最小多項式 $f(x)$ が与えられ, β の全ての共役元は, L の表現

$$L = K(\beta) \equiv K[x]/\langle f(x) \rangle$$

によって K 上の β の多項式として表されていることを意味する. ここで, 変数 x を β に割り当てている. また $\deg(f) = p$.

2.4.1 零でない Lagrange の分解式

$g_0(y)$ を $\mathbf{Q}$ 上の 1 の原始 p 乗根の最小多項式,$g(y)$ を $L = K(\beta)$ 上の 1 の原始 p 乗根の最小多項式とする. L と全ての 1 の p 乗根から生成される円分体 K' の合成体 (*composite field*) L' を構成する必要がある.



そのために, g_0 を $L = K(\beta)$ 上で既約因子に因数分解する; $g_0(y) = g_1(y) \cdots g_s(y)$. このとき,

補題 8 (1) 各 *1* の原始 p 乗根 ζ に対して $K' = K(\zeta)$ *and* $L' = L(\zeta)$

(2) K 上の g_0 の各既約因子はまた $L = K(\beta)$ 上の既約因子である. さらに,K 上の $g_0(y)$ の全ての既約因子 $g_i(y)$ は同じ次数を持つ.

補題 8 (2) より各既約因子 g_i, $i = 1, \cdots, s$ について剰余環 $R_i = K[x, y]/\langle f(x), g_i(y) \rangle$ は, 合成体 K' に同型な体になる. したがって, この剰余環 R_i によって 合成体 L' を表せる. さらに, 次の分解が得

られる.

$$R_0 = K[x,y]/\langle f(x), g_0(y)\rangle = R_1 \oplus \cdots \oplus R_s.$$

各 ζ に対して Lagrange の分解式 $u(\beta,\zeta)$ を構成する. すなわち, 各剰余環 $R_i = K[x,y]/\langle f(x), g_i(y)\rangle$ で $u(x,y)$ を構成する. Lagrange の分解式について

補題 9 (1) $u(x,y) \neq 0 \in R_i$ なる i が存在する. とくに,g_0 が K 上既約であれば, 全ての *1* の原始 p 乗根 ζ について $u(\beta,\zeta) \neq 0$.

(2) ある *1* の原始 p 乗根 ζについて $u(\beta,\zeta) = 0$ ならば, $u(\beta,\zeta^s) \neq 0$ なる p より小さな正の整数 s が存在する. ここで,ζ^s もまた *1* の原始 p 乗根である.

この補題 9 より必要な (零でない Lagrange の分解式を与えるような) 1 の原始 p 乗根 ζ_p は必ず見つかる. ここでは (1) のような ζ が見つかったとしよう. このとき, ある i に対し $g(y) = g_i(y)$ で, $L' = R_i = K[x,y]/\langle f(x), g(y)\rangle$ となる. そして, z を L'における (零でない) Lagrange の分解式 $u(x,y)$ に割り当てる. $u(\beta,\zeta_p)^p$ は L' において容易に計算でき, K 上の $\zeta_p(=y)$ の多項式 $H(\zeta_p)(=H(y))$ として得られる. L' 上の z の 最小多項式 $h(x,y,z)$ は $z - u(x,y)$ であり, z はまた $K(\beta)/K$ の原始元なので, $K(\zeta_p)$ 上の z の 最小多項式は $z^p - H(y)$ である. そして, このとき次が成り立つ.

$$L' = R_i \equiv K[x,y,z]/\langle f(x), g(y), h(x,y,z)\rangle \equiv K[y,z]/\langle g(y), z^p - H(y)\rangle.$$

2.4.2 ベキ根表現の具体的構成法

次に, 原始元を Lagrange の分解式とある 1 の原始 p 乗根の多項式として表すことを考える. そのための方法としてはいくつか考えられる.

方法 2§*1.2* で述べた方法を直接用いる方法が考えられる. これは,*1* の n 乗根のベキ根表現を構成する際に特に有効である *([2],[4] 参照)*. この方法では,“ 求められたベキ根表現中に現れてくるいくつかの $p-1$ 乗根に対してどの値をとれば良いのか? ” という問題が起こる. すなわち, あるベキ根に対する任意の値付け *(evaluation)* が許されない場合がある.

一般に, $\sqrt[m]{a}$ は多価函数であり, その値の選び方によってベキ根表現は他の元を表現するという場合がある. ここで, ベキ根表現に対して以下の概念を定義しておく.

定義 3ある代数的元を ξ , その最小多項式を φ とする. このとき, ξ のベキ根表現 $R(\xi)$ が,$R(\xi)$ の中に現れるベキ根の値のどの選び方に対しても最小多項式 φ の根を表すとする. このとき, ベキ根表現 $R(\xi)$ は強ベキ根表現 *(*strong radical representation*)* という.

ここで, もう一度整理すると問題は「$f(x), g(y)$,$h(x,y,z)$ から x を y と z の多項式として表した $x = P(y,z)$ を求める.」となる. この視点から,Gröbner 基底の計算を用いた方法, 代数拡大体上の GCD 計算を用いた方法が考えられる. Gröbner 基底の計算における基底変換 (*basis conversion*) を用いた方法について述べる. 代数拡大体上の GCD 計算を用いた方法については [4] を参照.

仮定 3 *1* の原始 p 乗根は既にベキ根表現されているとする.

方法 3 この *3* つの多項式から得られる拡大体は

$$K(\beta, \zeta_p) \equiv K[x, y, z]/\langle f(x), g(y), h(x, y, z)\rangle.$$

このとき, $f(x), g(y), h(x, y, z)$ はそのままでイデアル $\langle f(x), g(y), h(x, y, z)\rangle$ の辞書式順序 $x \prec y \prec z$ での簡約された *Gröbner* 基底になっている. *(*三角形式 *triangular form)* 剰余環が体なので, このイデアルは極大イデアルであり, 根基に一致する. x が y と z の多項式で書けるというのは, 言い換えると, $x - A(y, z)$ という形の元がイデアルに存在するということである *(*ここで,A は y と z の多項式*)*. よって, 辞書式順序 $z \prec y \prec x$ *or* $y \prec z \prec x$ *(*すなわち *block order* $\{z, y\} \prec\prec x$*))* で *Gröbner* 基底を計算すれば, $x - A(y, z)$ は *Gröbner* 基底による M-簡約によって 0 に簡約されなければならない. x は $x - A(y, z)$ の 頭項 *(head term)* なので, この *Gröbner* 基底に $x - P(y, z)$ という形の元が存在する. この元が x のベキ根表現を与える.

定理 10 $f(x)$, $g(y)$, $h(x, y, z)$ で生成されるイデアルの *block order* $\{y, z\} \prec\prec x$ での *Gröbner* 基底の中に元 $x - P(y, z)$ が存在する.

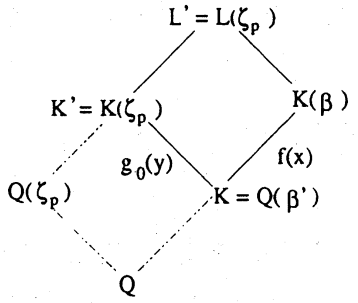
2.5 各原始元のベキ根表現

前節で一般的な形で述べた巡回拡大に対する方法を, 各拡大の原始元 β_i, $i = 1, \cdots, r$ のベキ根表現の構成に適用する. もちろん, 次を仮定する.

仮定 4 全ての原始元 β_i は計算されている.

2.5.1 強ベキ根表現

実際には強ベキ根表現を構成するのが目標であるので, ここで, 強ベキ根表現について触れておく. K は $\mathbf{Q}$ の有限次拡大で その原始元 β' と ζ_p は $\mathbf{Q}$ 上ベキ根表現されているとする.



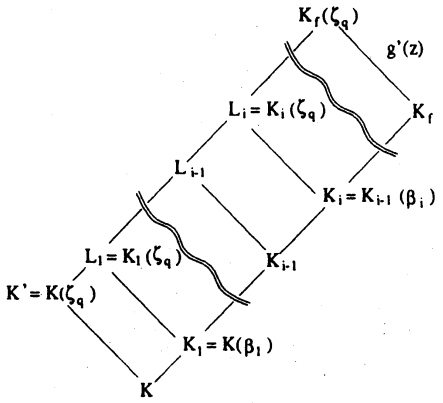
前節の方法で K 上の β の強ベキ根表現を求め, (β' と ζ_p の多項式として求まっている) β' と ζ_p をそれぞれそれらの $\mathbf{Q}$ 上の強ベキ根表現と置き換えると, $\mathbf{Q}$ 上の β のベキ根表現が得られる. 強ベキ

根表現について次が成立する.

補題 11 $\mathbf{Q}(\beta')(=K)$ と $\mathbf{Q}(\zeta_p)$ は 線形無関連 *(linearly disjoint)* だとする.(これは $g_0 = g$ という条件と等しい.) このとき,β のベキ根表現は, $\mathbf{Q}$ 上の ζ_p の強ベキ根表現と $\mathbf{Q}$ 上の β' の強ベキ根表現のどの組に対しても, 強ベキ根表現となる.

2.5.2 強ベキ根表現の構成

各拡大において 補題 11の条件を満たす, すなわち根の強ベキ根表現を構成するには, 基礎体をある円分体で置き換えればよい.



まず, 与えられた多項式 f によって決まる円分体 L を以下のように決める.

定義 4 $q_1, \cdots, q_s$ を $p_1, \cdots, p_r$ の中の異なる奇素数だとする. $q = \prod_{j=1}^{s} q_j$, $\zeta_q = \prod_{j=1}^{s} \zeta_{q_j}$ とする. このとき,ζ_q は 1 の原始 q乗根であり, 円分体 $\mathbf{Q}(\zeta_q)$ は全ての ζ_{p_i} そして $-1 = \zeta_2$ を含む. この円分体は $\mathbf{Q}(\zeta_q)$ は f に対応する円分体という.

ζ_q の (強) ベキ根表現は $\zeta_{q_1}, \cdots, \zeta_{q_s}$ の (強) ベキ根表現の積として与えられることに注意する. ζ_q のベキ根表現が必要だがそれについては次を仮定する.

仮定 5 ζ_q の強ベキ根表現は得られている.

変数 z を ζ_q に割り当てる. $g(z; y_1, \cdots, y_t)$ を K_f 上の ζ_q の最小多項式とする. ここで, $t = n$ or ℓ である. この多項式は $\mathbf{Q}$ 上の ζ_q の最小多項式 g_0 を分解体 K_f 上で因数分解することで得られる. (この因数分解の効率化については [4] を参照.) このとき, 全ての計算は $\mathbf{Q}(\alpha_1, \cdots, \alpha_t, \zeta_q) = K_f(\zeta_q)$, の上で行なわれ,$K_f(\zeta_q)$ は剰余環

$$\mathbf{Q}[y_1, \cdots, y_t, z]/\langle f_1(y_1), \cdots, f_t(y_1, \cdots, y_t), g(z, y_1, \cdots, y_t)\rangle$$

として表される.

i 番目のステップについて考える. まず,K_i を $L_i = K_i(\zeta_q)$ に換える. 変数 $u_1, \cdots, u_i$ を $\beta_1, \cdots, \beta_i$ にそれぞれ割り当てる. また Lagrange の分解式 $u(u_i, z)$ に変数 v を割り当てる. すなわち, 以下の多項式を考えるのである.

$$\begin{cases} u_j - \beta_j(y_1, \cdots, y_t) & j = 1, \cdots, i \\ f_k(x_1, \cdots, x_k) & k = 1, \cdots, t \\ v - u(u_i, z) & \\ g(z; y_1, \cdots, y_t) & \end{cases}$$

そして, ここで L_{i-1} 上での β_i のベキ根表現を考える.

ベキ根表現を求める前に注意すべきことがある. $|K_i : K_{i-1}|(= p_i)$ が素数であることから $|L_i : L_{i-1}| = p_i$ あるいは $L_i = L_{i-1}$ が成立する. さらに, 次が成立する.

補題 12

(1) $L_r = K_r(\zeta_q)$ は $\mathbf{Q}$ 上の *Galois* 拡大 であり, また $L_0 = \mathbf{Q}(\zeta_q)$ 上の *Galois* 拡大.

(2) L_r/L_i の *Galois* 群は G_i の中の ζ_q の固定群である. すなわち, $\{\sigma \in G_i | \sigma(\zeta_q) = \zeta_q\}$.

(3) β_i は L_{i-1} 上の L_i の原始元.

(4) $L_{i-1} \neq L_i$ ならば, L_i/L_{i-1} の *Galois* 群は K_i/K_{i-1} の *Galois* 群と同型であり,

よって 剰余群 G_{i-1}/G_i と同型.

よって,$L_i = L_{i-1}$ かどうかを決めなくてはいけない. これも,Gröbner 基底の基底変換の技法を用いて実行できる. block order $\{z \prec u_1 \prec \cdots \prec u_{i-1}, \prec u_i\} \prec\prec \{y_1, \cdots, y_t\}$ で簡約された Gröbner 基底を求めればよい. これは §3 と同様の議論より成り立つ次の補題による.

補題 13 *Gröbner* 基底 GB 中に, 変数 $u_j, \cdots, u_1, z$ の u_j $(j = 1, \cdots, i)$ について *monic* な多項式 $P_j(u_j, u_{j-1}, \cdots, u_1, z)$ が存在する. この P_j は $L_{j-1} = K_{j-1}(\zeta_q)$ 上の β_j の最小多項式である. また, $\mathbf{Q}$ 上の ζ_q の最小多項式 g_0 が GB 中に現れる. よって,

$$L_i \equiv \mathbf{Q}[u_{i-1}, \cdots, u_1, z]/\langle g_0, P_1, \cdots, P_i \rangle .$$

$L_i = L_{i-1}$ なのは P_i が u_i について線形なときに限る. もし P_i が u_i について線形だとすると, u_i すなわち β_i は$\beta_1, \cdots, \beta_{i-1}$ と ζ_q の多項式として表されている. β_i のベキ根表現は得られている訳である. したがって,$|L_i : L_{i-1}| = p_i$ のときに限りさらなる (基底変換を用いた) 手続きが必要になる. まとめると,

方法 4 $L_i = L_{i-1}$ かどうかまず決め, $L_i = L_{i-1}$ であればそのステップは終了, $|L_i : L_{i-1}| = p_i$ であれば, 以下の手続きを実行する.

多項式環 $\mathbf{Q}[y_1, \cdots, y_t, z, u_1, \cdots, u_i, v]$ の $u_1 - \beta_1, \cdots, u_i - \beta_i, v - u(u_i, z), f_1, \cdots, f_t, g$ によって生成されるイデアル $\tilde{\mathcal{J}}$ $\tilde{\mathcal{J}}$ は $\mathbf{Q}[y_1, \cdots, y_t, z, u_1, \cdots, u_i, v]$ の極大イデアルであり, その剰余環は K_f に等しい. また,$f_1, \cdots, f_t, g, u_1 - \beta_1, \cdots, u_i - \beta_i, v - u(u_i, z)$ は辞書式順序 $y_1 \prec \cdots \prec y_t \prec z \prec u_1 \prec \cdots u_i \prec v$. で, *Gröbner* 基底を作っている. このとき, 順序を *block order* $\{\{z, u_1, \cdots, u_{i-1}, v\} \prec u_i\} \prec\prec \{y_1, \cdots, y_t\}$, に変えることで *(*基底変換*),*$u_i$ のベキ根表現が, $u_1, \cdots, u_{i-1}, v, z$ の多項式として得られる.

注意 2 もちろん, 円分体の決め方は他にいくつか考えられる.

強ベキ根表現を与える他の方法としては, 各ステップで部分体に必要な原始元を添加する方法がある. すなわち, $L_0 = K_0(\zeta_{p_1})$, $\cdots$, $L_i = L_{i-1}(\beta_i, \zeta_{p_{i+1}})$ とするのである. この方法では, 各 i 番目のステップで L_{i-1} 上の β_i の最小多項式と $L_{i-1}(\beta_i)$ 上の ζ_{p_i} の最小多項式を求める必要がある.

また, 強ベキ根表現を与えるとは限らないが, 各 i 番目のステップにおいて K 上の 1 の原始 p_i 乗根の最小多項式, あるいは,$K(\beta_{i-1})$ 上の 1 の原始 p_i 乗根の最小多項式を用いても同様の方法が考えられる. これらは 疑強ベキ根表現 *(nearly strong radical representation)* とでもいえる *([4]* 参照*)*.

2.6 実験

実際に 富士通情報研で開発中の Risa/Asir [15] にインプリメントしいくつかの例について計算した結果を示す. 計算時間のデータは秒で与えられている. 計算機は RISC NEWS (R4000 50Mhz) を使用した. 例として以下の 10 個の可解な多項式を用いる. これらは,(4′) 以外は [3] において用いた多項式と同じものである. 以下の表で " *total* " は各拡大に対して結果を得るのに要する時間とその他必要な計算 (例えば $g(z)$ の構成など) に要する時間の合計である.

(4′) $x^5 - 5x^3 + 5x - 5$

(10) $x^6 + x^3 + 7$

(11) $x^6 - 3x^4 + 1$

(12) $x^6 + x^4 - 9$

(15) $x^6 + x^4 - 8$

(17) $x^6 + x^4 - x^2 + 5x - 5$

(19) $x^7 + x^6 - 12x^5 - 7x^4 + 28x^3 + 14x^2 - 9x + 1$

(24) $x^7 + 7x^3 + 7x^2 + 7x - 1$

(25) $x^7 - 14x^5 + 56x^3 - 56x + 22$

(26) $x^7 - 2$

部分体を構成するのに要した時間を表 1 に示す. 表は左から, 群の位数, 各拡大の拡大次数, 逐次原始元を用いた場合 (方法 1) に要した時間, 絶対的原始元を用いた場合に要した時間 を表す.

各原始元のベキ根表示を構成するのに要した時間を表 2 に示す. 表は左から, 逐次原始元を用いた場合 (注意 2 の擬強ベキ根表現を用いた) に要した時間, 絶対的原始元を用いた場合 (注意 2 の擬強ベキ根表現を用いた) に要した時間, 逐次原始元を用いた強ベキ根表現 (方法 4) に要した時間を表す.

ここで, "—" は 1 時間で結果が得られなかったことを示す. "*" は, 体の列 L_i の *contraction* が起こっていることを示す. すなわち,$L_{i-1} = L_i$. また,"▷" のついたステップでは *contractible root* が存在することを示す. (contractible case については [3] 参照.) このとき, 前のステップで根のベキ根表示は得られているので実はこの先は計算する必要はない.

表 1. 部分体

	ord.	deg.	suc.	abs.
(11)	18	3	0.19	0.30
		2	0.23	0.47
		3	0.29	0.38
total			0.71	1.15
(12)	24	3	0.18	0.24
		2	0.10	0.14
		2	0.12	0.25
		2	0.11	1.54
total			0.52	2.17
(15)	36	2	1.64	1.64
		2	0.57	0.65
		3	0.17	0.24
		3	0.18	1.30
total			2.56	3.84
(17)	48	2	1.51	1.56
		3	0.19	0.29
		2	0.19	0.98
		2	0.25	3.12
		2	0.24	17.18
total			2.38	23.14
(19)	72	2	51.16	52.28
		2	12.76	13.42
		2	13.89	67.57
		3	12.52	449.80
		3	24.78	1971.46
total			115.13	2554.53

表 2. ベキ根表現

	ord.	deg.	suc.	abs.	strong
(11)	18	3	1.68	3.18	0.78
		2	0.60	1.12	* 0.25
		3	2.94	7.85	1.23
total			5.23	12.15	4.17
(12)	24	3	0.60	1.01	0.44
		2	0.12	0.4	0.42
		2	0.11	0.28	▷ 0.28
		2	0.20	1.27	▷ 0.29
total			1.03	2.96	5.05
(15)	36	2	0.05	0.23	0.29
		2	0.16	0.47	* 0.18
		3	0.60	3.03	1.94
		3	1.59	2.46	▷ 1.07
total			2.43	6.20	46.45
(17)	48	2	0.17	0.52	0.53
		3	0.45	3.80	0.53
		2	0.20	1.59	0.69
		2	0.27	37.25	▷ 0.81
		2	0.35	3.6	▷ 1.03
total			1.47	46.77	63.49
(19)	72	2	0.53	0.66	2.94
		2	0.58	9.55	2.09
		2	2.85	703.84	47.31
		3	19.41	—	21.50
		3	18.12	/	▷ 20.96
total			41.50	—	7108.03

次に,10 個の多項式に対する時間データを表 3 に挙げておく. ただし, 部分体の計算は逐次原始元を用いた方法 1 を, ベキ根表現については, 逐次原始元を用いた場合 (注意 2 の擬強ベキ根表現を用いた) の方法を使った. これらの計算中で必要とされる Gröbner 基底の計算は辞書式順序で実行したが, 表 3 で "∘" は§5.2 で述べた block ordering を用いることで高速化を図れた.

表 3

	ord.	deg.	subfield	radical
(4′)	20	2	2.15	1.30
		2	4.48	0.44
		5	2.04	47.30
total			8.68	52.69
(10)	12	3	0.04	0.41
		2	0.07	0.10
		2	0.08	0.09
total			0.20	0.60
(11)	18	3	0.19	1.68
		2	0.23	0.60
		3	0.29	2.94
total			0.71	5.23
(12)	24	3	0.18	0.60
		2	0.10	0.12
		2	0.12	0.11
		2	0.11	0.20
total			0.52	1.03
(15)	36	2	1.64	0.05
		2	0.57	0.16
		3	0.17	0.60
		3	0.18	1.59
total			2.56	2.43

	ord.	deg.	subfield	radical
(17)	48	2	1.51	0.17
		3	0.19	0.45
		2	0.19	0.20
		2	0.25	0.27
		2	0.24	0.35
total			2.38	1.47
(19)	72	2	51.16	0.53
		2	12.76	0.58
		2	13.89	2.85
		3	12.52	18.41
		3	24.78	18.12
total			115.13	41.50
(24)	14	2	0.67	0.53
		7	2.49	2385.43
total			3.17	2386.11
(25)	21	3	3.75	19.36
		7	13.79	∘ 2819.27
total			17.54	2838.63
(26)	42	3	0.75	2.24
		2	0.75	1.96
		7	0.53	33.03
total			2.03	37.24

計算結果の例 (11) $x^6 - 3x^4 + 1$ を例にとる. 各ステップについてリスト [K_{i-1} の逐次最小多項式 β_i , K_{i-1} 上の K_i の 原始元 β_i] が得られる. 変数 $u_1, \cdots, u_{i-1}, v$ が $\beta_1, \cdots, \beta_{i-1}, \beta_i$ にそれぞれ割り当てられている. 分解体 K_f は 2 根 a, b 添加 で得られる.$K_f = \mathbf{Q}(a, b)$. a と b の定義多項式は $f_1 = a^6 + a^3 + 7, f_2 = b^3 + a^3 + 1$.

```
[405] series_pe_suc(GS,TP,RS,PPP);
<Extension Step,1>
[-v^3-21*v^2+609*v+6461,-6*b*a^2-6*b^2*a-7]
0.19sec
```

```
<Extension Step,2>
[2*v^2-2*u1*v-13*u1^2-162*u1+9693,-9*a^3+6*b*a^2-12*b^2*a-8]
0.23sec
<Extension Step,3>
[-v^3+u2,-a+2*b]
0.29sec
710msec + gc : 170msec
```

方法 4 によって得られた強ベキ根表現については結果だけ示す. ここで,q は 3 であり,$g(z;a,b) = z - \frac{1}{3}a^3 + \frac{1}{3}$. $L_1(= K_1(\zeta_3))$ は $L_2(= K_2(\zeta_3))$ と一致する. よって, 第 2 ステップでは Lagrange 分解式を計算する必要はなく所要の結果はここで得られる.

$$
\begin{aligned}
u_1 &= -\frac{1}{126}v_1^2 z - \frac{1}{378}v_1^2 + \frac{1}{3}v_1 - 7 \\
u_2 &= (\frac{1}{9}u_1^2 + \frac{11}{9}u_1 - \frac{719}{9})z + \frac{1}{18}u_1^2 + \frac{10}{9}u_1 - \frac{719}{18} \\
u_3 &= \frac{1}{3}v_3 \\
v_1 &= \sqrt[3]{122472z + 81648} \\
v_3 &= \sqrt[3]{(3u_1^2 + 33u_1 - 2157)z + \frac{3}{2}u_1^2 + 30u_1 - \frac{2157}{2}} \\
a &= -\frac{1}{271674}(7u_1^2 - 2110u_1 - 22529)v_3 z + (44u_1^2 - 326u_1 - 38116)v_3 \\
b &= \frac{1}{543348}(7u_1^2 - 2110u_1 - 22529)v_3 z + (44u_1^2 - 326u_1 + 52442)v_3
\end{aligned}
$$

参考文献

[1]穴井 宏和 , 横山和弘 . (1992) 多項式の可解性の判定 - 多項式の可解性とその可解性判定アルゴリズム- ワークショップ「数式処理」会議録 (於 日本大学) 84-99.

[2]穴井 宏和 , 横山和弘 . (1993) ベキ根による方程式の解の構成 -1 の原始 n 乗根の構成- ISIS Research Report 93-5J.

[3]Anai, H., Noro M., Yokoyama K. (1994). Computation of the splitting fields and the Galois groups of polynomials. presented at MEGA '94 (also submitted to the proceedings).

[4]Anai, H., Yokoyama K. (1994). Radical Representation of Polynomial Roots. ISIS Research Report 94-13E.

[5]Atkinson, M. D. (1975). An Algorithm for Finding the Blocks of a Permutation Group. *Math. Comp.* **29**, 911-913.

[6]Becker, T., Weispfenning, V. (1993). *Gröbner Bases*. Springer-Verlag, GTM 141.

[7]Buchberger, B. (1985). *Gröbner bases: an algorithmic method in polynomial ideal theory*, *Multidimensional System Theory*, Reidel Publ. Comp., pp. 184-232.

[8]Butler, G. (1991). *Fundamental Algorithms for Permutation Groups.* Lect. Notes in Comp. Sc., **559**, Springer-Verlag.

[9]Dixon, J. (1990). Computing subfields in algebraic number fields. *J. Austral. Math. Soc. (Series A)* **49**, 434-448.

[10]Ford, D.J., McKay, J. (1989). Computation of Galois groups from polynomials over the rationals, *Computer Algebra*, Lect. Notes in Pure Appl. Math., **113**, pp. 145-150.

[11]Furst, M., Hopcroft, J., Luks, E. (1980), Polynomial-Time Algorithm for Permutation Groups. *Proc. Twenty-first Annu. IEEE Sympos. Found. Comput. Sci. 1980*, pp. 36-41.

[12]Kolesova, G., McKay, J. (1984). Practical strategies for computing Galois groups, *Computational Group Theory*, Academic Press, pp. 297-299.

[13]Landau, S., Miller, G. L. (1985). Solvability by radicals is in polynomial time. *J. Comput. System Sci.* **30**, 179-208.

[14]Lang, S. (1965). *Algebra.* Addison-Wesley.

[15]Noro, M., Takeshima, T. (1992). Risa/Asir – a computer algebra system. *Proceedings of International Symposium on Symbolic and Algebraic Computation 1992.* New York: ACM Press, pp. 387-396.

[16]Sims, C. C. (1970). Computational methods in the study of permutation groups. *Computational Problems in Abstract Algebra*, Pergamon, Elmsford, pp. 169-183.

[17]Soicher, L. H. (1984). An algorithm for computing Galois groups. *Computational Group Theory*, Academic Press, pp. 291-296.

[18]van der Waerden, B. L. (1991). *Algebra I.* Springer-Verlag.

[19]Yokoyama, K., Noro, M., Takeshima, T. (1989). Computing Primitive Elements of Extension Fields. *J. Sym. Comp.* **8**, 553-380.